10. Enterprise Management

This chapter includes the enterprise management organization, information system monitoring and controls, integrated network management, and proposed measures of effectiveness for the information infrastructure. The relationship of this chapter with the ITSG is shown in Figure 10-1.

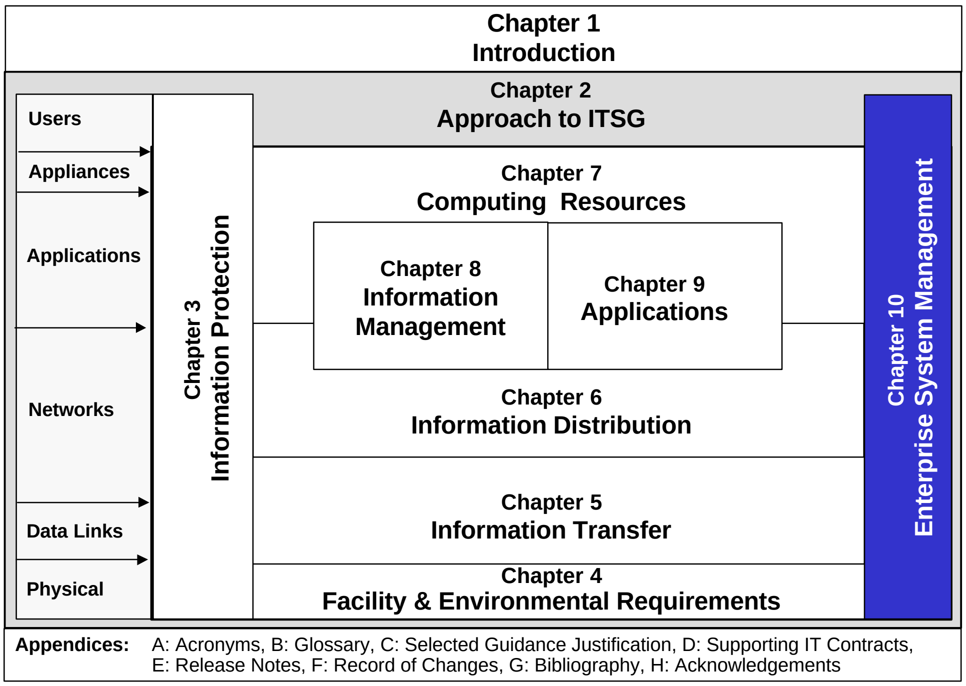

Figure 10-1. ITSG Document Map highlighting Chapter 10, Enterprise Management

10.1 Introduction

Enterprise management encompasses information systems and integrated network management. Enterprise management supports procedures and tools that maintain the integrity and efficiency of IT resources. The procedures and tools support proper planning, configuration, and problem solving. Network and cable management, resource management, systems administration, and security systems all fall within the scope of enterprise management.

The enterprise management framework provides the following:

- Integrated approach to managing diverse networks and information systems
- Environment for developing and integrating management applications
- Structure in which management applications can operate consistently
- Basis for delivering IT services to customers according to predefined levels
- Features provide a flexible and scalable platform for managing change, complexity, and cost-of-ownership

Management of the entire IT spectrum is needed to achieve the seamless, single-system performance of the complete Naval enterprise called for under the DON CIO management strategy. Information systems include those components required to provide voice, audio, video, imagery, and data services to our customers. In presenting the standards guidance, this chapter includes a proposed integrated management strategy for the entire information infrastructure – including applications and computing resources. Rationale: standards for enterprise management can have little relevance unless there is a DON enterprise strategy for providing these services to an integrated Naval information infrastructure. Enterprise management is a critical part of the infrastructure foundation.

Enterprise management encompasses enterprise-wide organization, systems monitoring, control, and quality. Each of these elements is addressed to orchestrate the implementation of information technologies throughout the DON infrastructure. Enterprise management is similar to information protection in that it spans all technology layers (Figure 10-1). Addressing system control and quality together connects the infrastructure control mechanisms (system control) and the infrastructure feedback (system quality) providing a complete control-response loop.

Figure 10-2 illustrates the context for system control and quality over a representative architecture. System monitoring or control processes must be present in each system component of the architecture from the appliances in each local area network to the network node devices in each wide area network.

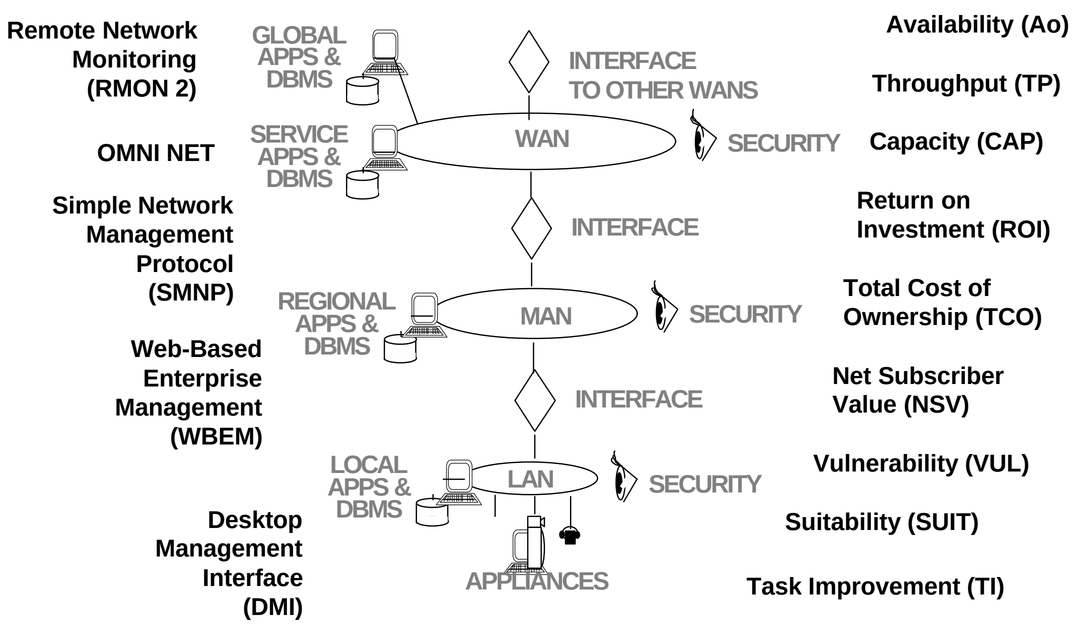

Figure 10-2. Enterprise Management Standards and Guidance in the context of the enterprise system architecture

Enterprise system control and quality measurement is impossible without an organizational structure that permits assignment of responsibility for system monitoring, control, and quality. The organizational structure has assigned enterprise management functions at appropriate commands in order to aggregate system metrics for total system quality. The next section of this chapter outlines an organizational management framework.

- Section 10.1 - Overview
- Section 10.2 - Organizing for Enterprise Management
- Section 10.3 - System Monitoring and Control Standards Guidance
- Section 10.4 - System Quality

10.2 Organizing for Enterprise Management

The enterprise management organization must support the full scope of services and systems. It must address the current system implementation, as well as the evolution of the infrastructure and applications as technologies and command missions change.

Best Practices

The Navy and the Marine Corps will establish an integrated community of Information Technology Service Centers (ITSCs) that support warfighters, operational users, and support personnel by implementing, operating, and managing the DON's comprehensive information infrastructure. This infrastructure includes all systems that transport, process and store information including tactical and non-tactical; classified and unclassified; voice, video and data systems. Systems that comprise the infrastructure will be integrated to the maximum extent practical so that operators view the infrastructure as a single system covered by a single support group.

Recommended Implementation

The following provides the guidance and concept for managing the DON's enterprise information infrastructure.

10.2.1 Enterprise Management

There are multiple dimensions of enterprise management that must be understood to adequately address the full scope of functions performed, objects managed, and level of management focus. To accomplish this we introduce and define three dimensions of enterprise management for the purpose of addressing enterprise management standards.

- Enterprise Management Functions
- Enterprise Component Categories
- Command Echelon/Area of Geographic Coverage

10.2.1.1 Enterprise Management Functions

Table 10-1 outlines the enterprise management functions that must be supported.

System Implementation	System Operations	System Support
Configuration Management	System Control	Personnel
System Architecture	System Configuration	Accounting
Systems Engineering	Storage Management	Asset Management
Systems Integration	Fault Management	Administration
System Analysis	Performance Management	Billing
Cost Analysis	Security Management	
Acquisition	Help Desk	
Installation	Service Desk	
Testing	Logistics Support	
Training		

Table 10-1. Enterprise Management Functions

10.2.1.1.1 System Implementation

System implementation includes functions that prepare and implement changes to the DON enterprise technical infrastructure. It includes management of cable plant, hardware devices, software licenses, network services, circuit provisioning, commercial applications and tactical/business applications. The support organization will provide orderly system changes and implementation.

Industry standards have yet to address the greater role of system implementation and configuration management software, hardware, and network resources. The X.700 (OSI) Software Management function and POSIX 1003.7 provide software administration and distribution guidelines.

10.2.1.1.2 Systems Operations

Systems operations includes eight functions that support and control the currently implemented infrastructure.

10.2.1.1.2.1 System Control

System control involves taking specific action against network and system components to change their status. This includes controlling the configuration and definition of the resources. Control of the network from a workstation, control of the network configuration, controlling remote processors, and controlling operating system resources are all examples of system control. Note that realtime dynamic control of resources in tactical networks, e.g. aboard ship, is best handled locally and is generally not feasible or practical to accomplish from a centralized, infrastructure-wide system control mechanism.

10.2.1.1.2.2 Systems Configuration

The Systems Configuration will address elements such as moves, adds and changes occurring in the user population. No industry standard yet exists.

10.2.1.1.2.3 Storage Management

Storage management provides for the backup and recovery of systems through system and network data collection and logging. Storage management protects critical data stored, including all database and application backups, from unauthorized use, overwriting, or deletion. It automatically archives data before you run out of disk space, and transparently restores the data when you need it.

- Hierarchical storage management features will also be provided. Dynamic placement of data across various storage technologies, such as memory, disks, and tapes, based on usage and retention parameters

10.2.1.1.2.4 Fault Management and Performance Management

Fault management involves fault identification, isolation, recovery, resolution, and message filtering. The system must identify and correct systems faults at control centers before the user detects the problem. Faults identified by users must be acted upon and solved promptly. A tracking system will allow the user to determine the status of problem resolution.

Performance management involves the continuous monitoring of system performance. It requires trend analysis as well as system modeling and simulation to determine when system upgrades are required. Control centers should have remote monitoring and diagnosis capabilities on wide area network equipment that address both the network and end-user equipment.

X.700 (OSI) standards exist for fault management and performance management. Also, TOG's XIMS defines many operational services such as alarm, event, and scheduling management.

10.2.1.1.2.5 Security Management

Security management addresses access to the system including user accounts, certificate administration, firewall management, encryption, system certification and accreditation support. Security management must provide solutions for information-at-rest as well as information-in-transit, and must account for emerging requirements for multiple release categories such as NOFORN, NATO, coalition partners, Partners for Peace, etc. The ITSC organization (discussed in Section 10.2.2.1) will implement intrusion detection systems, perform vulnerability assessments and provide malicious code (virus) detection. The organization will establish a reporting scheme so that detected and user-reported security incidents are promptly acted upon by the security or law enforcement agency.

For information about security, see Chapter 3, Information Protection.

10.2.1.1.2.6 Help Desk and Service Desk Customer Interface

The ITSC Help Desk is the front line interface to the users to resolve issues associated with IT services. The Service desk is the front line outreach center to minimize disruption to user operations during system upgrades and configurations changes. The Service Desk supports change control, coordination, approval, and implementation.

Both the Help Desk and the Service Desk require a standard customer interface. The customer interface function collects requirements from and coordinates with the users of services. User requirements include change requests, requests for additional services, requests for new services, and problem requests. The consumer interface function tracks requests and problems until resolution and provides feedback to the users. No industry standard exists at this time.

10.2.1.1.2.7 Logistics Support

Applications are available to track inventory of IT consumables and provide notice when it is time to reorder. The IT Logistic Support System should be coupled with the Asset Management System. No standard yet exists.

10.2.1.1.3 System Support

The five functions under the system support category are personnel, accounting, billing, asset management, and administration. Of these, ITSG standards guidance is applicable to accounting, asset management and billing.

10.2.1.1.3.1 Accounting

Accounting maintains costs and expenses associated with the use of IT resources. Advanced accounting capabilities support a breakdown of the use of shared resources. Accounting also encompasses software metering.

Both X.700 (OSI) and TOG's XRM define accounting standards.

10.2.1.1.3.2 Asset Management

Asset management provides a repository of accurate and timely data about managed resources. Inventories are used to track expected occurrences of the resources against the actual existence of the resources. Inventories may also include various reference information such as location, owner, or supplier contact.

No industry standards exist for this function.

10.2.1.1.3.3 Billing

A modern billing capability must be provided for those shore/base enterprise environments that use the MAN/WAN facilities of telecommunication service providers. The fundamental function of a billing system is to provide Navy and Marine Corps service centers with an invoice for telecommunication provider network usage and support Naval business and cost of operation objectives. This capability need not be provided for Navy and Marine Corps owned and operated networks in the shipboard environment.

No industry standards exist for this function.

10.2.1.2 System Component Categories

The following outlines the system component categories that must be managed.

> **Appliances**. The hardware, software, and associated peripherals that the operator use to interface with the system. This includes computer clients, servers, printers, telephones, video teleconferencing (VTC) equipment, and associated software.

Communication Circuits and Equipment. The underlying communication circuits, cryptographic equipment, and termination equipment associated with the network. This includes terrestrial communications circuits, wireless (cellular) area coverage, line-of-sight radio, and Satellite Communication (SATCOM) as well as the associated radios, crypto, modems, CSU/DSU, and CODECs. This category focuses on layer 1 (physical) and layer 2 (data link) of the OSI model.

Network. The nodes and circuits that establish fault tolerant, interconnected paths between command elements. This includes the selection and configuration of routers, switches, gateways, bridges and associated addressing schemes and domains. This category focuses on layer 3 (network) and 4 (transport) of the OSI Model.

Basic Network and Information Distribution Services (BNIDS). The core services needed to provide basic information dissemination. This includes the selection and configuration of domain name services, directory services, web services, network news service, electronic mail, and file transfer methods. This and the remaining categories focus on the basic elements of layers 5 and up (session, presentation, and application) of the OSI Model.

Voice. Telephone equipment and services.

Video. Video teleconferencing (VTC) and television equipment.

Servers. Computers, including workstations and mainframes, that provide information services to a network.

Commercial Applications. Commercial software applications.

Operational Applications. Government developed tactical/non-tactical applications such as the Global Command and Control System (GCCS) or Global Combat Support System (GCSS).

10.2.1.3 Command Echelon / Geographic Area of Coverage

The command echelon and geographic area of coverage that must be supported are defined in the following:

Global. The collection of organizations that have enterprise-wide responsibilities. They include the Secretary of the Navy (SECNAV) Staff, the Chief of Naval Operations (CNO), the Commandant of the Marine Corps, the System Commands and Naval Bureaus.

Fleet/Theater. Organizations responsible for the underway fleet, deployed Marines, and theater forces. These include the Fleet Commander-in-Chief (CINC) associated force commanders and type commanders. (“Fleet” is used in lieu of “Fleet/Theater” for brevity throughout this chapter.)

Regional. Organizations responsible for the operations of primarily shore-based or in-garrison commands located within a wide geographic area.

Base, Post, Camp, Station. Organizations responsible for supporting commands within a local area or campus.

Unit. A command with an operational or support mission.

Element. Aircraft, other vehicles, or members of a unit that detach and conduct missions, operations, or support.

10.2.2 Concept of Operations

In the model below (Figure 10-3), rows represent system component categories and columns represent corresponding management functions that support each category. This support has to cover each command echelon from the global down to the command element.

Scale: Naval Fleet Regional Unit Element	OPERATIONS								IMPLEMENTATION										SUPPORT			
	Sys Control	Storage Mgt	Fault Mgt	Perf. Mgt.	Security Mgt.	Help Desk	Service	Logistics	Config Mgt	Sys. Engr	Syst. Arch.	Cost Anal.	Syst. Anal.	Syst. Intgr.	Acquisition	Implement.	Testing	Training	Accounting	Asset Mgt.	Admin	Personnel
Oper Apps																						
Coml Apps																						
Data Base Mgt																						
Video																						
Voice																						
Net Services																						
Network																						
Transmission																						
Appliances																						

Figure 10-3. Matrix of Enterprise Management Functions, System Component Categories and Geographic Coverage

The following items and succeeding paragraphs describe support for the enterprise management elements depicted in Figure 10-3.

- Information Technology Service Centers (ITSC)
- Integrated System Management Tools
- System Control and Maintenance
- Application and Information Service
- System Implementation Support

10.2.2.1 Information Technology Service Center (ITSC) Concept

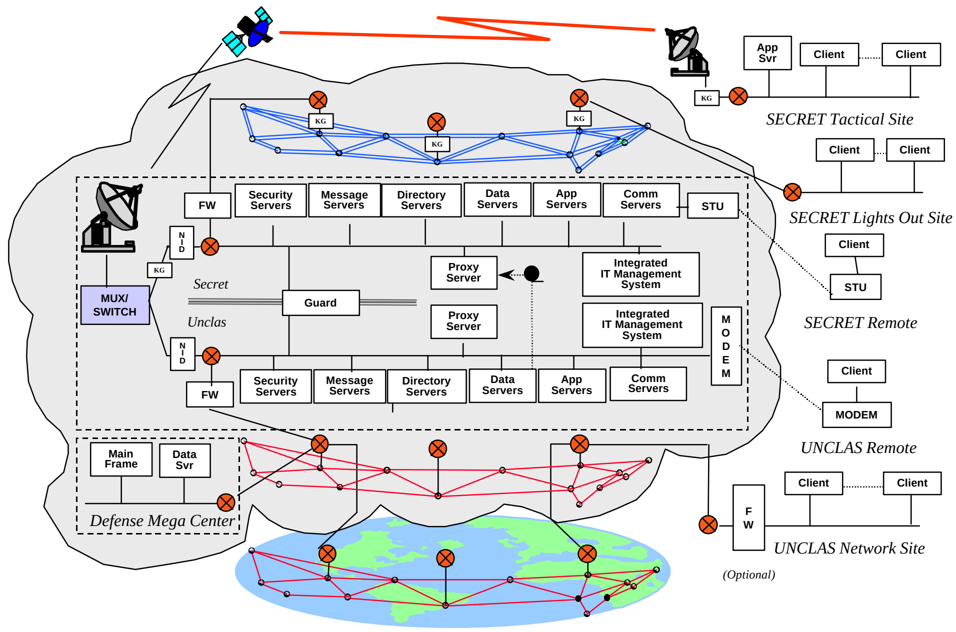

Figure 10-4. ITSC Functions Including Enterprise Management, Interface and Centralized Computing Services

An Information Technology Service Center (ITSC) would provide comprehensive IM/IT support to the DON IT infrastructure. This includes information system operation, implementation support, and administration for a community of information producers and consumers. The ITSCs would be “Local Control Centers” in full compliance with the Joint Defense Information Infrastructure (DII) Control Centers (CC) Concept of Operations (CONOPS). Figure 10-4 illustrates.

Each ITSC would perform three major duties:

- Integrated information system implementation, control and maintenance.
- Interface information flow from network to network including dial-in service.
- Consolidated information/application repository and distribution center for individual commands in the region.

10.2.2.1.1ITSC Framework and Scope of Coverage

To provide a framework for consolidation on a global scale, as well as services close to the user, enterprise coverage is described with varying scope of coverage. The ITSC goal would be to achieve efficiency through consolidation, but not at the expense of reliability and quality service.

Global Information Technology Services – Service to the entire enterprise. For fault tolerance, at least two sites need to provide global ITSC service.

Fleet/Theater Information Technology Services – Services to the fleet units that are primarily underway or deployed. These ITSCs will be aligned with the Fleet CINCs.

Regional Information Technology Services – Services that support all Naval commands within a geographic region. The majority of information service functions are included in the scope of this service.

Joint Information Technology Services – Services that support non-Naval commands within a concentration area primarily operated by the U.S. Navy or Marine Corps. Hawaii and Norfolk are examples of concentration areas for Naval-sponsored joint commands – USPACOM and USACOM.

Base Information Technology Services – These services would be an extension of the Regional Information Services where physical presence is required. Services in this echelon would be primarily hardware-related such as device and cable plant maintenance, component replacement, software distribution and dial-in service. Since these services need to be performed at remote locations, they would be designated as *Information Technology Outreach Centers* (ITOCs) and serve as the base "store front" for the ITSC.

10.2.2.2 Integrated Enterprise Management Tools

The Joint DII Control Centers CONOPS provides a description of the Joint DII Control System, which includes system element management systems, general system support tools, deployed system support tools and information assurance tools. Shown in Figure 10-5 is the Joint DII CONOPS model applied to the ITSC concept. On the left side in the vertical stack of boxes are the control and monitoring tools. These tools are associated with the technologies listed to their left and roughly align to the seven layer ISO model. Across the top are the security control and management tools. Across the bottom are the overarching enterprise management tools. All of the tools are focused by the Integrated Information Technology Management System (in the center of the diagram) that the ITSC system managers use to monitor and control.

All ITSCs will have access to all enterprise management tools in the Integrated Information Technology Management System, although the tools themselves will not be physically located at every ITSC. Economy-of-scale is achieved by a single global management system, however, quality service is normally best achieved when it is delivered directly to the customer. To optimize economy and quality, system elements that can be managed remotely will be managed centrally (e.g., trouble ticketing). Enterprise management elements that require physical presence will be performed locally. For example, ITSCs and ITOCs that require physical presence to troubleshoot and maintain systems would have the necessary management tools on location. As a general rule, software and network management tools would tend to be centralized at the global ITSC and hardware monitoring and diagnosis tools would be distributed to the localities(ITOCs).

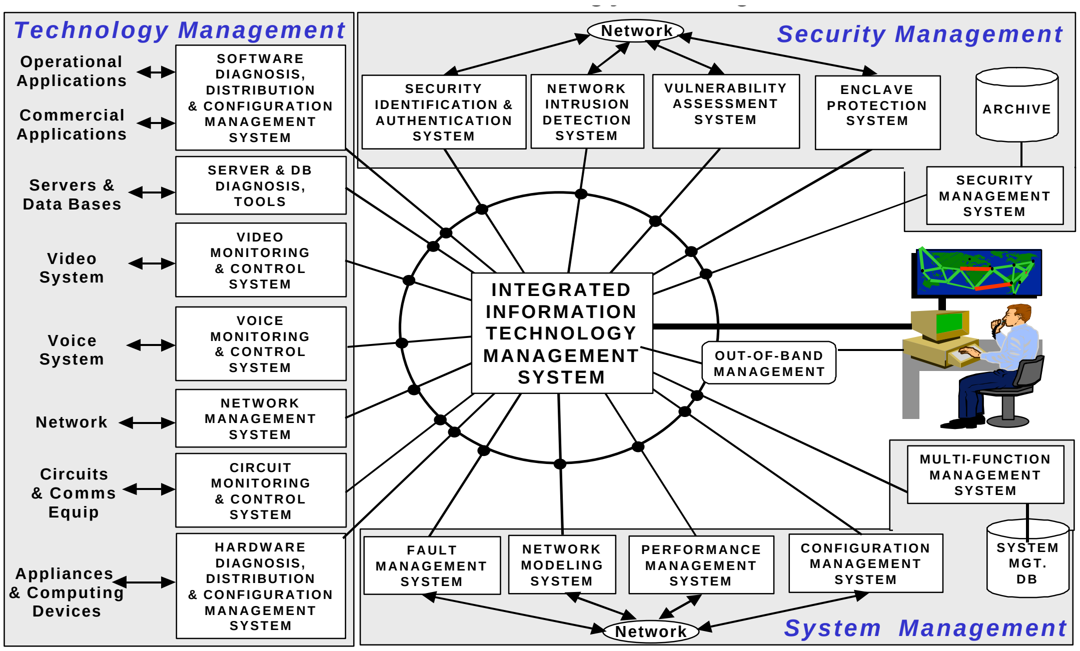

Figure 10-5. ITSC Information Technology Management Tools

10.2.2.3 System Control and Maintenance

ITSC staff personnel would use the Integrated Information Technology Management System to analyze the system performance for tuning and planning, and to monitor and respond to system faults. Trouble tickets will be provided to the appropriate system support activities that dispatch the resources to resolve problems.

10.2.2.4 System Implementation Support

A goal of the DON CIO is to achieve system integration by shifting from application-based enterprise management to infrastructure-based enterprise management. Instead of having a LAN, workstation and server for each application, the infrastructure is developed, supported and evolved as a single system. Traditional tactical/functional programs would transition from developing their own independent infrastructure to developing operational or business applications that utilize the infrastructure. Infrastructure components will be implemented in the same manner. Under the ITSC concept, a coordinated enterprise effort would support existing installations. System Commands and Naval Bureaus would continue to develop and acquire applications to install onto the infrastructure. In its fully realized form, the DON CIO would coordinate with the development and acquisition communities to stand up Integrated Product Teams (IPTs) that are responsible for developing, testing, installing, setting up training and logistic support of specific functional systems.

10.3 System Monitoring and Control Standards Guidance

Section 10.2.1.1 described the management functions as one dimension of total enterprise management. Monitoring and control specifications are needed to build tools and procedures to support these functions. Enterprise management specifications are just beginning to provide monitoring and control capability that support enterprise services.

Enterprise management specifications support both manager/agent and object-oriented management structures.

- The manager/agent structure represents a traditional approach with agents throughout the infrastructure that interact across consolidated, hierarchical monitor and control facilities, called managers.
- The object-oriented structure is an approach in which all resources, services, and management applications appear as objects and interact as peers. Using object orientation, differences among various technical elements may be abstracted so that information and control appear to be the same. For example, a common command is issued to query the status of a device. If that query is sent to an object representing the device, the object could internally perform the device-dependent query and translate the result into a commonly understood status.

Several standards continue to evolve. In the data networking area, Simple Network Management Protocol (SNMP), and Remote Network Monitoring 2 (RMON 2) standards are established and continue to proliferate in the United States in emerging products. Although version 2 of SNMP has been available for several years and addresses important issues of expanded security and performance, low industry acceptance has resulted because competing security approaches could not be resolved. Recent drafts of SNMP Version 3 (SNMP 3) contain security features that are expected to receive wide industry acceptance..

The RMON 2 specification is gaining popularity because it provides centralized enterprise management for complex networks with less network coordination than SNMP. The Desktop Management Task Force (DMTF) consortium is defining desktop APIs for monitoring and controlling personal workstation hardware and software resources. The resultant product is called the *Desktop Management Interface* (DMI). In the telecommunications area, the telecommunications management network (TMN) is the management architecture standard specified by CCITT/ITU-T. TMN is a basis for the internetworking of various network components and management systems for mainly public telecommunications networks.

The following provides guidance on enterprise management implementation of standards and specifications.

Best Practices

Use management systems and protocols that minimize non-payload overhead and that can be assembled into an integrated system to control and monitor all aspects of the entire infrastructure from a single workstation.

Recommended Implementation

	Current ITSG	Projected ITSG			
Not Recommended	**1999**	**2000**	**2001/2002**	**2003/2004**	**Emerging**
	SMNPv1 RMON 2 XSM	SMNPv1 RMON 2 XSM	SMNPv3 RMON 2 XSM	SMNPv3 RMON 2 XSM	DMI WBEM DMTF V2.0
Activities, Platforms, Operational Environments	ITSCs and Shore. Bandwidth consumption must be considered prior to use for Ships, Ground, and Aircraft				

Table 10-2. System Monitoring and Control Recommended Implementation

10.3.1 The X.700 Series and XSM

Of the few supporting standards supporting enterprise management functions, the most complete are the ITU-T X.700 series. While the X.700 is accepted by the ITU-T, the ISO and the IEC, commercial support of the X.700 is very limited. A declaration that X.700 series is the enterprise management standard would provide little support for advancing the DON towards system integration. The completeness of the X.700 series, however, makes it attractive as a potential standard. Figure 10-6 provides an overview of the X.700 series of enterprise management specifications. The most commonly used specification of the X.700 series is X.711, the Common Management Information Protocol (CMIP), which is comparable to the Simple Network Management Protocol (SNMP).

The X/Open System Management (XSM) by The Open Group (TOG) specification profile effort captures the X.700 series standards.XSM is a comprehensive framework for managing networks and systems from the perspective of the services they deliver to end customers. The goal is to facilitate the automation of information system service management while addressing legacy management system integration and transition to distributed management systems. XSM promotes management software that allows an administrator to manage heterogeneous systems networks as a single logical system.

OSI System Management Architecture

Title	ISO/IEC Designation	ITU-T Designation
OSI Management Architecture		
Management Framework for OSI	7498-4	X.700
Systems Management Overview (SMO)	10040	X.701
OSI Management Communications		
Common Management Information Service Definition (CMIS)	9595	X.710
Common Management Information Protocol (CMIP)	9596-1	X.711
CMIP PICS Proforma	9596-2	X.712
Basic Management Communications	AOM-11	
Enhanced Management Communications	AOM-12	
OSI Management Information		
Management Information Model	10165-1	X.720
Definition of Management Information (DMI)	10165-2	X.721
Guidelines for Definition of Managed Objects (GDMO)	10165-4	X.722
Requirements and Guidelines for Implementation Conformance Statement Proformas associated with OSI Management (MOCS Guidelines)	10165-6	X.724
OSI Generic Definitions – Systems Management Functions		
Object Management Function	10164-1	X.730
State Management Function	10164-2	X.731
Attributes for Representing Relationships	10164-3	X.732
Alarm Management Function	10164-4	X.733
Event Report Management Function	10164-5	X.734
Log Control Function	10164-6	X.735
Security Alarm Reporting	10164-7	X.736
General Management Capability	AOM211	
Alarm Reporting and State Management Capabilities	AOM212	
Alarm Reporting Capabilities	AOM213	
General Event Report Management	AOM214	
General Log Control	AOM231	
Security Audit Trail Function	10164-8	X.740
Objects and Attributes for Access Control	10164-9	X.741
Usage Metering Function	10164-10	X.742
Metric Objects and Attributes	10164-11	X.739
Test Management	10164-12	X.745
Summarization Function	10164-13	X.738

Title	ISO/IEC Designation	ITU-T Designation
Confidence and Diagnostic Test Categories	10164-14	X.737
Scheduling	10164-15	X.746
Management Knowledge Function	10164-16	X.750
Change-Over Function	10164-17	X.751
Software Management	10164-18	X.744
Domain Policy Management	10164-19	X.749
Time Management	10164-20	X.743
Generic Network Information Model		M.3100
Alarm Surveillance		Q.821
Performance Management		Q.822
Security Function Profiles	AOM24	
Metric Objects and Attribute Profiles	AOM22	
Summarization Function Profiles	AOM253	
Key: OSI – Open System Interconnect ISO – International Standardization Organization IEC – International Electrotechnical Commission ITU-T – International Telecommunications Union – Telecommunication Standardization Sector		

Figure 10-6. X.700 Series Specifications and Related ITU Proposals

10.3.2 Industry Specifications

Today’s networks are predominantly hybrids. Government and industry organizations are meshing managed services from public telecommunications providers with their own private enterprise networks to provide high quality service with fewer operational problems. No single management technology or specifications can deal with the complexity of the hybrid networks. Effective end-to-end management is achieved by selecting a combination of technologies that provides complete function coverage, wide commercial usage, and promise of technology support.

The appropriate management scheme is a combination of industry-proposed and vendor-specific specifications. SNMP and CMIP are the dominant network management protocols. SNMP and RMON2 are the primary specifications for network communications management, Desktop Management Interface (DMI) is appropriate for computing resource management, and Web-Based Enterprise Management (WBEM) is appropriate for internet-based network middleware services. CMIP is the network management protocol most widely promoted by the telecommunications industry. ITU-T Telecommunication Management Network (TMN) is the primary specification for the public data and voice telecommunications networks. Figure 10-7 shows these specifications as applied to the ITSC Information Technology Management Tools.

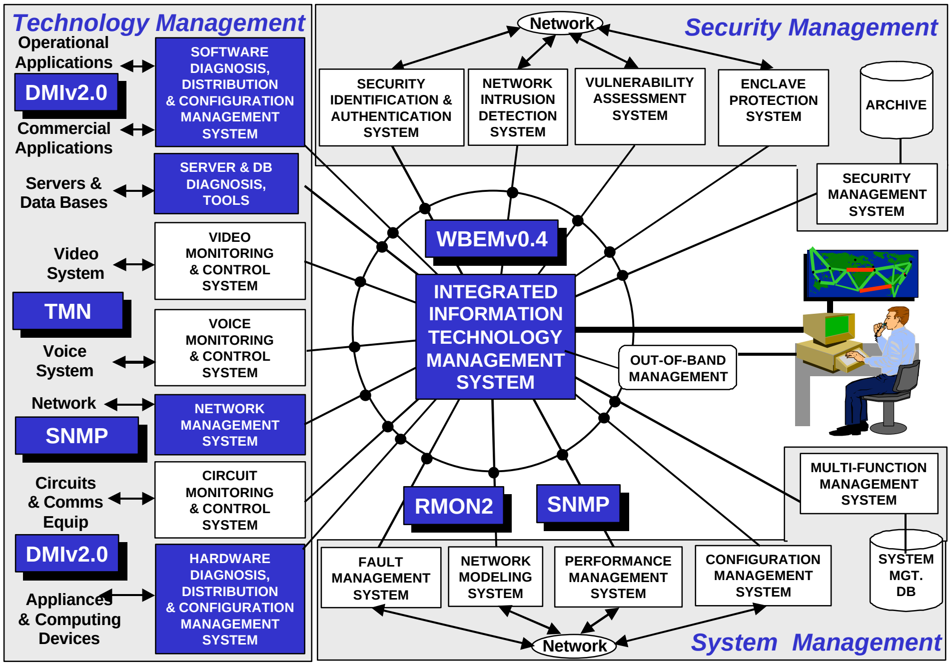

Figure 10-7. SNMP, RMON 2, WBEM and DMI relationship to the ITSC Information Technology Management Tools

10.3.2.1 Simple Network Management Protocol (SNMP).

SNMP version 1 (SNMPv1) is the JTA mandated standard for network management. The greatest advantage to SNMP is that its design is simple and expandable, and easy to implement on a large network. Originally intended as an interim network manager, wide usage of SNMP ensued before more advanced network management protocols such as CMIP appeared. Security concerns have been addressed in version 2 of SNMP (SNMPv2); however, SNMPv2, like CMIP, is neither simple nor in wide use. Although the JTA mandates SNMPv1, use of RMON 2, CMIP or SNMPv2 to avoid the security vulnerability of SNMPv1 is encouraged to build operational experience and offer a migration path from SNMPv1.

The output from the SNMPv2 Working Group did not become a widely accepted standard primarily because two competing security approaches could not be resolved. The SNMPv2 standard provides major improvements over SNMPv1 in two major areas that are important to the management of large enterprises. SNMPv2, through the GetBulk command, increases the amount of management data that can be transferred in a single transaction, thus reducing the potential for heavy data loads and provides a decentralized network management scheme that is useful in large networks where a centralized approach would be cumbersome at best.

Recently a draft standard for SNMPv3 was completed which includes the functionality of SNMPv2 and incorporates the security features found in the proposed security approaches. SNMPv3 includes 3 modules:

- The Message Processing and Control module handles SNMP message creation and parsing functions, and also determines if proxy handling is required for any SNMP message.
- The Local Processing module performs access control for variable binding data, processing that data and trap processing.

- The Security module provides authentication, and encryption functions, and checks the timeliness of certain SNMP messages.

Expectations are that SNMPv3 will succeed in the marketplace and products meeting this standard will now start to appear.

10.3.2.2 Remote Network Monitoring Version 2 (RMON2)

The RMON 2 specification supports monitoring of the network and network devices from selected nodes on the network. The distributed network monitoring and control capability allows more control over large, complex networks with less management overhead. System statistics can be accumulated by remote devices and uploaded to the primary management system upon demand. RMON2 provides an end-to-end view of the traffic flow across the global, enterprise network. It provides network statistics, packet filter, and capture for complete distributed protocol analysis, and provides statistics at the application layers of the protocol stacks. This capability gives the system manager better visibility of network assets.

10.3.2.3 Web-Based Enterprise Management (WBEM)

WBEM is the most promising specification for the Integrated Information Technology Management System (Figure 10-5 and Figure 10-7). Its web-based hypermedia interface is very attractive because of its comprehensiveness and flexibility. WBEM promises to support SNMP, DMI, and ultimately CMIP, as well as vendor-specific specifications. In addition to standard web specifications for HyperText Transfer Protocol (HTTP) and HyperText Markup Language (HTML), WBEM uses:

- HyperMedia Management Schema (HMMS) as an extensible data model representing the managed system environment.
- HyperMedia Managed Object (HMMO) as a managed entity that has data that can be either interrogated or managed by a browser either directly or through a management schema. Every framework object must have at least one URL.
- HyperMedia Object Manager (HMOM) as a management application that aggregates management data and uses one or more protocols to present a uniform representation to the browser using HTML. The HMOM could be implemented using existing development platforms such as Java, Active X, CGI, CORBA or COM. It provides a hierarchical control point for accessing and managing other HMMOSs on the network, services to manage large numbers of managed objects, gateway agents to map HTTP requests for the native protocol of the non-HMMO entities such as SNMP and DMI.

WBEM is considered to be an emerging standard with recommended compliance required for shore and ITSC operational environments. Bandwidth requirements must be assessed before WBEM is recommended for ship, ground, space, or air operational environments.

10.3.2.4 Desktop Management Interface (DMI)

DMI provides an interface between all computing resources (hardware, software, and peripherals) and the management system. It is designed to be independent of any specific computer, operating system or management protocol. It can be used locally, or remotely via a network using remote procedure calls. It is mappable to existing network management protocols including both SNMP and CMIP. DMI was developed by the Desktop Management Task Force (DMTF) and consists of the following elements.

- A format for describing management information
- A service provider access point
- Two sets of APIs to the service providers, one for the management application and a second for the components
- A set of services to facilitate remote management

10.3.2.5 Telecommunications Management Network (TMN)

Telecommunications carriers today must rapidly introduce and manage new competitive service offerings. This means quick integration of state-of-the-art communications equipment from multiple vendors. In response to the challenge of successfully integrating huge numbers of new network elements into the existing network, the carriers and international standards bodies have defined a solution called the "Telecommunications Management Network" or "TMN." TMN consists of a series of interrelated national and international standards and agreements which provide for the surveillance and control of telecommunications service provider networks on a worldwide scale. TMN also has applicability in wireless communications, cable television networks, private overlay networks, and a host of other large scale, high bandwidth communications networks. TMN provides for integrating new multi-vendor equipment with legacy systems within a common network management structure. The TMN architecture integrates management, service, and accounting functions in order to achieve higher service quality, reduced costs, and faster product integration. TMN eliminates competitive barriers by demanding that manufacturers open up their equipment by supporting a common management architecture. With the worldwide TMN acceptance by telecommunications and wireless carriers, equipment manufacturers must support TMN in order to remain competitive. The scope of TMN managed areas includes: switching networks, transmission networks, ISDN, B-ISDN/ATM, data networks, and mobile networks.

The TMN relevant standards are documented in the ITU M.3000 Series: M.3000 and M.3010 for TMN, and X.701 for OSI Management. The TMN architecture in M.3010 is defined from three perspectives: a physical architecture and an information architecture based on the manager-agent concepts of OSI systems management, X.701; a functional architecture describing layering of TMN management functionality; and the application of architecture to the management of various technologies (described in the following documents: SDH networks in G.784, switching in Q.513, SS7 networks in Q.750, and ISDN in M.3600).

Where additional TMN application functionality beyond that provided by existing OSI Management standards is needed, it is built on existing OSI capabilities provided by the OSI CMIS, X.710. Such enterprise management services in turn are mapped onto associated application protocol data units defined in the OSI CMIP, X.711, for transfer across TMN interfaces.

10.3.2.6 Emerging Management Efforts for Multimedia Networks

The emerging network management standards and products are being developed to provide an open framework, core services, and unifying applications that integrate voice, data, and mixed media network environments across multiple vendors and locations and give customers sophisticated, comprehensive, enterprise-level network management capabilities. In this environment, it appears that the computer communication and telecommunications network standards organizations will allow the SNMP and CMIP network management protocols to coexist.

For instance, the ATM Forum has been working on a series of network management standards for configuration management, fault management, and performance management. The ATM Forum network management standardization focuses on the management information base (MIB) specifications, which define managed objects and associated attributes that are necessary to implement various management functions. The keys to an open network management platform are a common communications protocol and a common set of managed objects or information elements to facilitate monitoring and control of ATM network elements. These are realized through a standard MIB.

In this context, there are a large number of relevant MIBs. MIBs are based on simple network management protocol (SNMP) or common management information protocol (CMIP) standards. Besides The ATM Forum MIBs (SNMP and CMIP), there are MIBs defined by other standards bodies including the Internet Engineering Task Force (SNMP), TOG (CMIP), and ITU-T (CMIP). In addition, there are proprietary MIBs developed by vendors to manage their switches (primarily SNMP-based). Even though each standards body has specific objectives, there is some overlap between MIBs developed by different standards bodies. Often, users need a combination of various MIBs to meet their requirements. To manage ATM networks, it is important to understand the applicable MIBs, their purpose, scope and inter-relationships.

10.3.2.6.1ATM Forum MIBs

As ATM technology goes across private networks and public networks, ATM network management has different perspectives depending on whether one is interested in managing the private or public networks or both. The ATM Forum has defined a generic model that encompasses both areas. Basically, the ATM Forum network management model defines five interfaces: M1, M2, M3, M4, and M5. Private ATM network management is addressed through M1 combined with M2. M1 is concerned with management of end user equipment connecting to either private or public switches, and M2 with management of ATM switches and networks. M3 is the link between private and public networks to exchange fault, performance and configuration information. M4 pertains to management of public ATM switches and networks. M5 supports interactions or exchange of management information between any two public networks.

10.4 System Quality

Implementations of IT infrastructure, systems and services should identify measures of quality that indicate levels of performance. Prior to initiating any IT implementation, initial planning to match and align the IT solution to support the organization’s functional missions is a crucial first step. That step should include measures of effectiveness for assessing resultant performance. During the subsequent development, implementation and operation of the IT system, the application of a consistent enterprise system quality framework is important. The prescribed set of measures include System Effectiveness, System Efficiency, System Characteristics, and System Behavior.

System Quality metrics can demonstrate the efficiency of the hardware and software infrastructure. Metrics are used in a wide range of activities – from validating acquisition effectiveness, to measuring central design performance, to allowing fine tuning of a system at the local level. The application of metrics across our diverse information systems represents a difficult task, one requiring focused management and special tools.

For all implementations, selecting the correct measurements, interpreting the data, and properly using the outcome is key to assessing performance. Prior to selecting any performance metrics it is important to understand how to measure, what to expect from the measurement, the cost of the measurement, and how it fits into the enterprise-wide mission.

10.4.1 System Quality Concept

For warfighting readiness, performance of our IT infrastructure, and return on our IT investment, it is important that we have measures of performance. Measuring the quality of the Naval information infrastructure, in aggregate, is a formidable task. Effective measures have not been determined. The IT infrastructure is owned and maintained by multiple, independent organizations, making aggregation of measures very difficult. Accurate inventories and configuration management data are inconsistently maintained. There is an absence of financial benchmarks on which to base return on investment calculations. The remainder of this chapter establishes a framework upon which to gauge the effectiveness and efficiency of the DON enterprise information infrastructure. The system quality metrics that are introduced enable assessment of IT support of the mission and provide feedback to the system control methods that support system configuration, operation, and implementation.

The system should be continually examined under demanding operational scenarios to verify its operational performance. The system should be stressed through exercises covering at least these three scenarios:

- A logistics operation (e.g., Desert Shield)
- A tactical operation (e.g., Desert Storm)
- A natural disaster (e.g., Provide Comfort)

System quality data should be collected and retained for statistical and trend analysis.

The dimensions to System Quality are explained using a simple model illustrated in Figure 10-8:

System Effectiveness – Metrics and attributes that describe how well the IT infrastructure helps customers perform their mission objectives and tasks. These metrics and attributes also identify the responsiveness of the infrastructure to emerging requirements.

System Efficiency – Metrics and attributes that provide the system costs to develop, implement, operate and maintain as a function of mission effectiveness.

System Characteristics –Attributes that describe the static condition of systems or system components after implementation or reconfiguration.

System Behavior – Metrics and attributes that show how the collection of system components are responding to usage and the current situation.

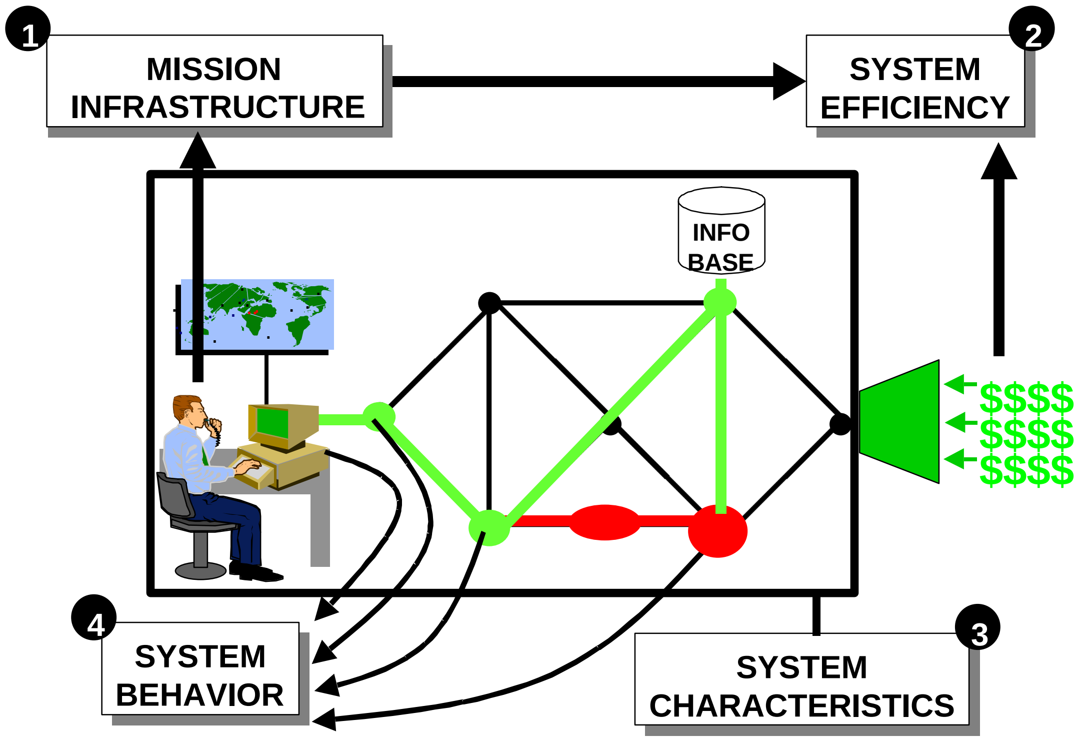

Figure 10-8. Systems quality dimensions

The Systems Characteristics dimension has a relationship with the three remaining dimensions. Varying the attributes of System Characteristics causes changes to System Behavior and System Efficiency (based on cost). These changes to System Behavior are further manifested in changes to System Effectiveness.

This model must be further developed to adequately measure quality on the complex system that comprises the DON enterprise information infrastructure. Of the four dimensions, System Effectiveness and System Efficiency can be measured independently of what is going on inside the individual Information System Domains (ISDs). System Behavior and System Characteristics are explained by events and data residing within each ISD; their measures can be obtained effectively only within an individual ISD, but any attempt to aggregate these rapidly gains complexity when crossing ISD boundaries.

However, System Behavior metrics, because of their ability to show response to operational conditions and system performance, must be aggregated to provide enterprise measures. The concept of coordinated ITSCs, with their enterprise management responsibilities and supported clientele help mitigate this complexity.

Infrastructure Effectiveness		System Characteristics	
System Performance		Block Diagram	BD
Suitability	SUIT	System Identifying Information	SII
Availability of Capability	AVC	Network Characteristics	NET
Vulnerability	VUL	Application Characteristics	APPS
Task Time	TT	Appliance Characteristics	APDV
Task Improvement	TI	Facility Characteristics	FAC
Capability Response	CR	Scalability	SCA
Information Quality		**System Behavior**	
Accuracy	ACY	Volume	VOL
Precision	PCN	Capacity	CAP
Error Rate	ER	Throughput	TP
Time-Late	TL	Throughput Rated	TP-R
Time Since Validation	TSV	Congestion	CG
Completeness	COMP	Blocking	BK
Duplication	DUP	Utility	UT
Accessibility Target	ACSY-T	Availability	Ao
Accessibility Actual	ACSY-A	Mean Time Between Failures	MTBF
System Efficiency		Mean Time to Repair	MTTR
Cost	COST	E-mail to No One	EMN
Total Cost of Ownership	TCO		
End-User Maintenance Cost	EUMC		
Subscriber Value	SV		
Net Subscriber Value	NSV		
Return on Investment	ROI		

Table 10-3. Dimensions of System Quality

Table 10-3 summarizes the system quality metrics that support the four dimensions – Infrastructure Effectiveness, System Efficiency, System Characteristics, and System Behavior. These metrics are described in the remainder of the chapter. Each of the four descriptions includes at least one summary table that follows the format of Table 10-4. The summary tables can be used by managers as work sheets to assess performance of these four dimensions.

System Quality Measurement	Abbreviation	Unit of Measure	Measurer
Title	Abbreviation	Unit of Measure	Who performs the Measurement
Description or formula for computation			

Table 10-4. System Quality Metrics Summaries (format)

10.4.2 System Effectiveness

The formulation of relevant, quantitative, timely, and universally applicable metrics of mission effectiveness for application to information infrastructure is very challenging. Development of these metrics is illustrated in Figure 10-9. Two tracks are shown, one that leads from the mission through organizational elements – functions, tasks and people; and the second that leads from the infrastructure through system elements – applications, networks and appliances. The first track must be understood to properly determine and apply the metrics obtained from the second track.

Appliances and people intersect to create the capabilities needed to accomplish the task. The figure shows the relationship between capabilities and requirements that feeds back to organizational functions and system applications. Capabilities lead to the following results: more information, better understanding, increased knowledge, greater productivity, good decisions, and proper directions as depicted at the bottom of the figure.

The infrastructure's contribution to producing the "Results" is measured by the System Performance and Information Quality. Both serve to enhance Infrastructure Effectiveness. The items under System Performance measure how well the system supports the task. The items under Information Quality measure the goodness of the system's product – information.

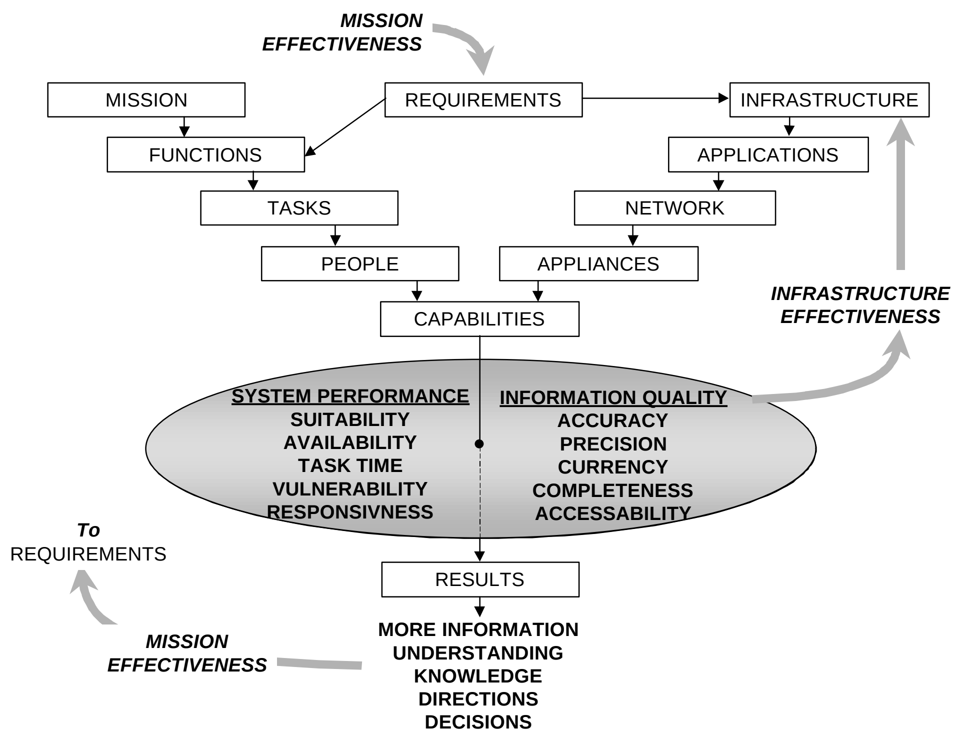

Figure 10-9. Relationship Between Mission and Infrastructure Effectiveness

10.4.2.1 System Performance

The measures of information system performance are as follows.

Suitability. How well system capability matches the required task – "Is the system doing the right job?" The system does several jobs, therefore suitability (expressed as a percentage) will be the number of tasks supported over the number of tasks expected to be supported by the system subscriber.

Availability. How much of the time the system capability can be expected to be present when it is needed. It is the total sum of time that each system capability is operable divided by the product of elapsed time and number of system capabilities.

Vulnerability. The ability to deny a service or obtain unauthorized access to information. It is measured by a vulnerability assessment team on an intrusive, but harmless, basis and recorded as number of intrusions per week. Associated details must be recorded and tracked as well.

Task Time. The length of time taken to complete a common, standard task. This provides a measure of productivity and improvement. Productivity increases as less time is taken to complete a task, so that more tasks can be completed within a given time. Improvement in task times before and after a system upgrade can be used to determine a percent enhancement (or decrement). The challenge is in determining common standard tasks.

Capability Responsiveness. The length of time it takes for a system to adapt and provide new or altered capability based upon emergent subscriber requirements. The units of measure would likely be in days and should be averaged over all capabilities provided or upgraded.

Quantifying these measures hinges on defining the functional system capabilities and common standard tasks.

10.4.2.1.1 Defining Required Functional System Capabilities

As discussed in Chapter 2, the four core capabilities for the infrastructure are: (1) command LAN and standard client personal workstations, (2) distributed communications to dispersed forces, (3) wide area network communications to shore and garrison forces, and (4) basic network and information distribution services (BNIDS). Functional capabilities -- common operational picture, employment scheduling, repair parts tracking -- are predicated on these core capabilities. Fleet Commander-in-Chiefs (CINCs) and the Marine Force Commanders will define required functional system capabilities that need to be measured and tracked.

10.4.2.1.2 Defining Common Standard Tasks

Likewise, “common standard tasks” need to be identified and selected. Candidates should be tasks that are performed frequently and don’t require substantial research or innovation, but nevertheless are essential to the organization’s mission. A representative common standard task is the creation and ultimate delivery of a Casualty Reports (CASREPs).

The CASREP requires diagnosis of a broken component and research to collect information that is transcribed into a message. The message is sent to a group of common CASREP recipients as well as recipients that need to know the readiness status of the unit. Once the CASREP message is received by supporting units, action and coordination ensues to solve the problem. This common standard task could be supported by a system capability that replaces the CASREP message with a trouble ticket system. The casualty reporting task would remain common but the data entry and transfer method would change. The affected unit would enter the data directly into the CASREP database. The information would then be automatically posted or routed to the supporting commands that need to take action.

The functional system capabilities and the common standard tasks will be identified and selected as the ITSG matures.

10.4.2.1.3 Calculating Suitability Metrics

Each command should provide input to the ITSC to develop a list of tasks expected to be supported by the information infrastructure. Supported tasks over the total expected supported tasks is the command's suitability (percentage). The command's suitability will be updated monthly by the servicing ITSC. The ITSC should collect suitability values from each command, then calculate mean, median, mode, standard deviation, variance and extreme values for the region. Fleet and Global ITSCs should determine the same suitability statistics by echelon, geographic area, and platform type. These statistics should be calculated monthly and analyzed for trends. The resultant analysis should be used to guide and prioritize information technology implementation.

10.4.2.1.4 Calculating Capability Availability Metrics

Each command should help the ITSC identify important information system capabilities required for mission support — both organic (locally owned and operated) and remote. Capability examples include commercial items such as word processing or electronic mail as well as operational items such as automated message handling or common operational picture. ITSCs will maintain comprehensive lists of these functional capabilities. Capability outages, assessed locally or identified by client commands, will be tracked by the ITSCs. The availability of the command's information infrastructure (AVC) for the month is as follows:

$$\text{AVC} = \frac{\text{(NUMBER OF Capabilities) * (Elapsed Time) –} \atop \text{Sum of elapsed time of capability outages}}{\text{(NUMBER OF Capabilities) * (Elapsed Time)}}$$

Servicing ITSCs should determine each command's monthly AVC. The ITSC should also collect AVC for the region and calculate mean, median, mode, standard deviation, variance and extreme values. Fleet and Global ITSCs should determine the same AVC statistics by echelon, geographic area, and platform type. Analysis of this data should be used to guide and prioritize information technology implementation.

10.4.2.1.5 Determining Vulnerability

Vulnerability (VUL) is determined by and ITSC vulnerability assessment team and is the number of penetrations achieved over a week. The vulnerability assessment team should frequently probe the information infrastructure with intrusive but harmless efforts to gain access or identify areas where disruption could occur to system devices from external sources.

The full description of the penetration method and associated system vulnerability should be recorded and tracked. The collection and analysis of these measures shall be highly restricted but provided as needed to information system managers and commanding officers so that corrective action can be taken.

VUL = Number of penetrations per week

Vulnerability data should be collated by systems and echelons. ITSCs should perform associated statistical and trend analysis.

10.4.2.1.6 Calculating Task Time

Common tasks identified by the command should be measured to determine the average time required to execute. The task time sampling frequency is at command discretion . Task times (TT) should be collected by the ITSC for performance of standard statistical. Task times should be calculated after system upgrades to determine task improvement (TI) with the following calculation:

$$\text{Task Improvement} = \frac{\text{Old Task Time - New Task Time}}{\text{Old Task Time}}$$

10.4.2.1.7 Determining Capability Responsiveness

To measure capability responsiveness the new requirement must first be validated and sponsored by the appropriate authority. Upon commitment of funding (if required) the clock starts and runs until the capability is satisfactorily delivered by the system developer. Capability Responsiveness (CR) is the elapsed time from funding to system implementation as defined by the system developer expressed in elapsed work days. The Global ITSC should calculate and maintain mean, median, mode, variance, standard deviation and extreme value analysis as well as trend analysis.

10.4.2.1.8 System Performance Summary

Table 10-5 provides a summary of system performance metrics for mission effectiveness discussed.

System Quality Measurement	Abbreviation	Unit of Measure	Measurer
Suitability	SUIT	Percent	Command Consumer
$\text{SUIT} = \frac{\text{Number of Supported Tasks}}{\text{Number of Tasks Expected to be Supported}}$			
Availability of Capability	AVC	Percent	Command Consumer
$\text{AVC} = \frac{\text{(NUMBER OF Capabilities) * (Elapsed Time) – Sum of elapsed time of capability outages}}{\text{(NUMBER OF Capabilities) * (Elapsed Time)}}$			
Vulnerability	VUL	Events per week	ITSC
Determined value. Number of events per week with descriptions			
Task Time	TT	Time (minutes)	Command Consumer
Measured Value. The average amount of time that is takes to do a common standard task. Task must be specified for comparison with like tasks.			
Task Improvement	TI	Percent	Command Consumer
$\text{Task Improvement} = \frac{\text{Old Task Time - New Task Time}}{\text{Old Task Time}}$			
Capability Responsiveness	CR	Time (work days)	System Developer
Measured Value. Elapsed time from funding to capability delivery.			

Table 10-5. System Performance Metrics Summary

10.4.2.2 Information Quality

Information is the ultimate product of the information infrastructure. Measuring the quality of the product is essential to gauging the infrastructure's support to the mission. Information quality – accuracy, precision, and currency – measure the goodness of the individual information elements. Completeness, duplication and accessibility measure the goodness of information sets.

> **Accuracy**. The probability that the value is correct. Expressed as a percent, it is calculated by dividing the total number of correct values by the total number of values. It can also be expressed as an error rate equal to the number of errors over the total number of values. It can also be a pure probability calculated through statistical methods.
>
> **Precision**. The fidelity, granularity or relevance of the information. It is expressed with the same unit of measure as the data element itself as a plus or minus tolerance within which the value is accurate.
>
> **Currency**. The elapsed time from the creation, discovery or validation of the information to the present time.
>
> **Completeness**. The number of information elements in the information base as a function of the total number of information elements in the entire set. Completeness is expressed as a percentage.
>
> **Duplication**. The percentage of duplicate data elements in the information set.
>
> **Accessibility**. The degree in which the information stored or computed within the infrastructure is available to the target subscriber. The metric should be time measured from when a subscriber initiates a search until the time information retrieval starts. It measures the combination of subscriber training, information organization, and system response.

Of the measures, the information producer must measure accuracy, precision, and completeness. The ITSC may coordinate an independent assessment if requested by the subscribers. The subscriber, or ITSC representing a subscriber, measures timeliness and accessibility. The ITSC should also maintain statistics and trend analysis for each information set.

10.4.2.2.1Determining Information Accuracy and Precision

Information accuracy and precision go together. The accuracy of the information is dependent upon the stated precision. For example, the phrase "drive a car to work" is less precise than, but no less accurate than "drive a Volvo to work."

The information manager calculates the information accuracy (ACY) by performing a periodic assessment of the entire data set. The percentage is derived by subtracting the number of incorrect data elements from the total and then dividing by the total to obtain the percentage. In lieu of counting the total number of data elements (as attached to a particular task or functionality), a statistical sample set can be used to obtain a 95 percent confidence level at the precision level determined by the information manager or producer.

Information that requires a very high level of accuracy can be measured as an error rate (ER), where ER is a ratio of errors to the total number of data elements.

Information precision in a range or set of values that describe the detail or fidelity of the information. This level of fidelity is often determined by the capability of a sensor. The precision should be varied as necessary to ensure the accuracy level does not drop below a selected value. Most information should be maintained at a precision level that keeps accuracy above 99.9 percent with the most accurate data having an error rate or less than one per million. Precision is measured as a tolerance (plus or minus from the expected value) or a range (he set that contains the expected value to include the value itself). Precision can be varied depending on the mission element.

Information accuracy and precision should be computed monthly and submitted to the ITSC.

10.4.2.2.2 Calculating Information Currency

Information currency is either time-late (TL) for dynamic information, or the elapsed time since validation (TSV) for static information. Time-late is the time difference between time of the discovery or data creation, and the present time. Elapsed time since validation is the difference between the present time and the last validation time provided by the information producer or manager.

10.4.2.2.3 Determining Information Completeness

Completeness is the percent of data elements present in the information base over the number of data elements in the complete set. The information producer or manager calculates information completeness (COMP) first by determining the complete set of data elements present. Completeness should be determined by information production commands on a periodic basis with assistance from the ITSCs.

10.4.2.2.4 Determining Information Duplication

Duplication (DUP) is a negative measure that provides an indication that data base management needs improvement. It is proposed in order to put the “completeness” measure in perspective since data duplication can make a data base appear to be more complete. Duplication is the number of repeated occurrences of unique data elements divided by the total number of data elements. Duplication should be determined by the information production commands as needed for internal quality control. If required by information consumers, an independent measure of duplication by the ITSC can be performed and tracked.

10.4.2.2.5 Calculating Information Accessibility

There are two metrics associated with accessibility: target accessibility (ACSY-T) and actual accessibility (ACSY-A). The information producer or manager determines target accessibility. The manager makes the information accessible based upon the level of training and security access of the target information consumer. Target accessibility equals the sum of the data query time and the system expected response time. Actual accessibility is equal to the elapsed time from the start of the search to the start of the information download.

The ITSC must determine the cause of excessive ACSY-A with possible solutions being a system tune or operator training. In the case of ACSY-A where information cannot be retrieved, the ITSC must determine if the information is even available, and if not, determine if system capability should be upgraded. In this case, ‘system performance’ measures would be used (system capability response).

10.4.2.2.6 Information Quality Summary

Table 10-6 provides a summary of information quality metrics for mission effectiveness discussed.

System Quality Measurement	Abbreviation	Unit of Measure	Measurer
Accuracy	ACY	Percent	Producer Manager
$ACY = \frac{\text{Complete Number of Data Elements – Number of Incorrect Data Elements}}{\text{Complete Number of Data Elements}}$			
Precision	PCN	Units of Associated Information	Producer Manager
Determined value. Tolerance within which an information element value is expected to fall or the description of the set of items in which the information element value is contained.			
Error Rate	ER	Errors per number of elements (million)	Producer Manager
$ER = \frac{\text{Total Number of Errors in the Period of Time}}{\text{Total Number of Data Elements in the Period of Time}}$			
Time-Late	TL	Time (minutes)	Command Consumer
TL = Present Time - Data Time Stamp or Time of Event			
Time Since Validation	TSV	Time (days)	Command Consumer
TSV = Present Time - Time Stamp at Validation			
Completeness	COMP	Percent	Producer Manager
$COMP = \frac{\text{Number of elements present in the information base}}{\text{Total Number of information elements in the complete set}}$			
Duplication	DUP	Percent	Producer Manager
$DUP = \frac{\text{Number of duplicative data elements}}{\text{Total Number of information elements in the complete set.}}$			
Accessibility - Target	ACSY-T	Time (seconds)	Producer Manager
Measured Value. Elapsed time from start of an information query until the retrieval of the information as measured by the information producer or manager.			
Accessibility - Actual	ACSY-A		Command Consumer
Measured Value. Elapsed time from start of an information query until the retrieval of the information as measured by the information consumer or supporter.			

Table 10-6. Information Quality Metrics Summary

10.4.3 System Efficiency

Efficiency is the amount of effectiveness or productivity over the amount of resources (money or time) expended. This section focuses on financial resources (time resources are addressed under mission effectiveness because reducing the response time is the force multiplier that information provides infrastructure to the mission.)

System efficiency is a universal focus addressed predominately by commercial industry and normally includes two primary measures — “Total Cost of Ownership” (TCO) and “Return on Investment” (ROI). Both TCO and ROI are difficult to measure within the DON — TCO because of the fractionated information system implementation and ROI because the DON does not use profit as the primary measure of “return”. TCO and ROI as applied to the DON are addressed in this section.

10.4.3.1 Total Cost of Ownership (TCO)

TCO includes aggregating costs over the enterprise and aligning the cost categories with the infrastructure management system. Using this alignment, costs that appear to be out of line with expected values can be quickly investigated and corrected. Figure 10-10 shows a method for organization, categorization and aggregation. The ITSCs should compile and aggregate their data at each echelon on a monthly and annual basis. The tables are divided into several sections. The upper section provides display of costs for upgrade, technology refreshment, or migration of the infrastructure. The bottom section contains the cost breakdown for operations, maintenance, and support.

10.4.3.1.1 End-User Maintenance Cost (EUMC)

The ITSC mission is to minimize the amount of time that end users spend solving their own problems, although at times it is unavoidable. Commands that care to report this measure can do so under the metric End-User Maintenance Cost (EUMC). The EUMC is equal to the hourly rate multiplied by the number of hours spent troubleshooting and repairing a system. This performance measure is often attributable to the amount of resources provided to the organization. In some cases, it may be more economical to let users repair their own problems. This measure provides a methodology to guard against potential shifts in cost from the supporter to the user after reductions in infrastructure support resources. Costs passed to the end user can be tracked so that resources can be managed to minimize the total cost.

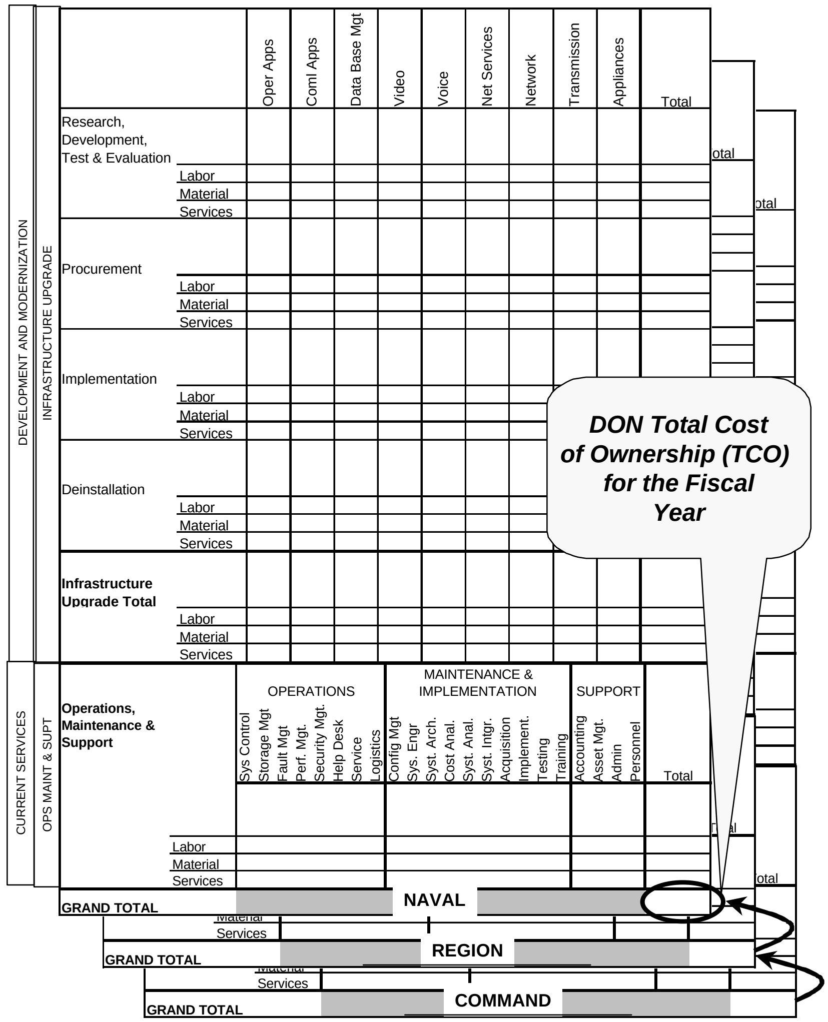

Figure 10-10. Aggregation of Costs to Provide the Total Cost of Ownership

10.4.3.1.2 Technology Refreshment and Infrastructure Upgrade Costs

In the above figure, infrastructure upgrade is broken down into four categories, with each subdivided into labor, material and services subcategories for greater detail. Across the top are columns that span the system component categories depicted in the rows of the enterprise management matrix, Figure 10-3. These costs are summed for each row and column over each echelon (command, region, Naval).

Research, Development, Test and Evaluation (RDT&E). The government has a significant role to play in researching and developing new information technologies. However, with the wealth of information technology resources in commercial industry, it is preferable to procure rather than develop. The focus has shifted from developing new technologies to testing and evaluating commercial products for integration into the Naval information infrastructure.

Procurement. Costs associated with systems, components and services to upgrade the infrastructure.

Implementation. Costs associated with the installation, integration, training, initial supply associated with the integration of a developed or procured system.

Deinstallation. Costs associated with the removal and disposal of obsolete or unneeded components.

10.4.3.1.3 Operations, Maintenance and Support

The bottom quarter of Figure 10-10 contains cost categories for Operations, Maintenance and Support (OM&S). As shown, the same cost categories of labor, material, and services are used as in the infrastructure upgrade section. The columns of the OM&S section match the enterprise management functions from the columns in Table 10-4.

10.4.3.2 Return on Investment (ROI)

TCO Section (10.4.2.1) and optional EUMC Section (10.4.2.2) provide the investment information needed for the ROI measure. Return can be measured using any of the system performance measures described in the mission effectiveness Section (10.4.1.1). The usefulness of ROI as a system efficiency measure greatly increases if a monetary value can be placed on system return. In a business sense, the customer provides revenue that generates a return (profit) after costs. The customers of the DON information infrastructure are the information consumer and information producer who rely on the infrastructure for receipt and delivery of information. Because the customer does not have to pay for any infrastructure benefit, an artificial value, related to mission effectiveness, can be assigned to the customer's beneficial use of infrastructure services.

10.4.3.2.1 Net Subscriber Value (NSV)

If a part of the infrastructure fails or if a service does not provide utility, a number of subscribers are impacted. The value of the information service to the subscriber is directly impacted by the time being spent using the system. The cost of downtime to a subscriber is the value of the subscriber's time lost due to non-availability of the system. Conversely, if the system shortens a task-time by allowing the user to more productively perform a task, then the value of the user's time gained is credited to the information system. To represent the value of the subscribers time (work-hours), the subscriber dollar value per hour (determined by the local comptroller) is multiplied by a utility factor and a mission criticality factor.

Subscriber Value (SV) = ($50) * Utility Factor * Criticality Factor

Where:

- $50 per hour is an arbitrary value chosen for the value of a subscriber's time
- Utility Factor is estimated percentage of time required to be spent on the service for the subscriber
- Criticality Factor is a percentage that expresses how critical a capability is relative to the command's mission.

Net Subscriber Value (NSV) = Sum of all associated Subscriber Values

ITSCs will assist Commanding Officers in establishing a utility factor and criticality factor for each information system capability and in determining the number of subscribers. ITSCs will aggregate the subscriber values for each capability, each system and system component that comprise the information infrastructure.

As a result, the ITSCs not only have a monetary value of a capability, but also a monetary value for the down time of a system component. For example, the cost associated with an out of service client PC would be less than that of a server based on relative net subscriber value. Use of net subscriber value will be factored into architecture decisions when determining the degree of system component redundancy for fault tolerance.

The total ROI for the infrastructure is the net subscriber value for all system capabilities divided by the Total Cost of Ownership (TCO). The ROI can also be calculated for each of the Systems component capabilities. Add the applicable SV(s). Determine the percent these SV(s) are of the total NSV. Multiply the OM&S total by that percent to equal the approximate amount of OM&S associated with those capabilities.

10.4.3.2.2 System Efficiency Summary

Table 10-7 provides a summary of system efficiency metrics as discussed above.

System Quality Measurement	Abbreviation	Unit of Measure	Measurer
Cost	COST	Dollars	Developer ITSC
Costs collected and collated by technology refreshment, operations, maintenance and support. Cost categories include labor, material, and services. For technology refreshment, subcategories include RDT&E, Procurement, Implementation, and Deinstallation. Cost also collated by technology and function.			
Total Cost of Ownership	TCO	Dollars	ITSC
Total aggregated costs of technology refreshment and operations, maintenance and support rolled up from commands into regions, regions into the Naval enterprise. Funds are also rolled up temporarily by month, quarter and fiscal year.			
End-User Maintenance Cost	EUMC	Dollars	Command Consumer
EUMC = Hourly Rate of the Subscriber * Time Spent Troubleshooting and Repairing the System			
Subscriber Value	SV	Dollars	Command Consumer
SV = Hourly Rate * Utility Factor * Criticality Factor			
Net Subscriber Value	NSV	Dollars per service or component	ITSC
NSV = Sum of all SVs associated with a service, capability, or component			
Return on Investment	ROI	Percent	ITSC
$\text{ROI}=\dfrac{\text{NSV for applicable capability, service system, or component (or any combination thereof)}}{\text{Net COST of applicable capability, service system, or component (or any combination thereof)}}$			

Table 10-7. System Efficiency Metrics Summary

10.4.4 System Characteristics

System characteristics measures are the controlling factors that determine the mission effectiveness and system efficiency measures discussed in the prior sections. System characteristics are simply the configuration of the information system domain.

10.4.4.1 System Configurations

The following is the minimum configuration items to be tracked by the ITSC to measure system characteristics. These items must be kept up-to-date.

System Block Diagram

System Identifying Information

- Domain Name
- IP Addresses
- ATM NSAP Addresses

Network Characteristics

- Number and Description of External Interfaces
  - WAN Service Providers
  - Communication Servers
  - Virtual Networks
- Network Topology
  - Network Diagram
  - Number and Description of Internal Network Nodes
  - Network Diameter expressed in Number of Nodes
  - Description of Cable Plant
  - Network Protocols Used

Application Characteristics

- Number and Description of Servers
  - Function
  - Processor(s)
  - Clock Speed
  - Memory
  - Storage
  - Operating System
  - Maximum Subscribers
- Commercial Application Software
  - Function(s)
  - Product
  - Vendor
  - Subscribers
  - License Information
  - Server Information
  - Maximum Subscribers

- Operational Application Software
    - Function(s)
    - Product
    - Developer
    - Sponsor
    - Subscribers
    - License Information
    - Server Information

Appliance Characteristics

- Number and Description of Computer Clients
    - Function
    - Processor(s)
    - Clock Speed
    - Memory
    - Storage
    - Maximum Subscribers
- Commercial Application Client Software
    - Function(s)
    - Product
    - Vendor
    - Operational Application Client Software
    - Function(s)
    - Product
    - Vendor
    - Number and Description of VTC Clients
    - Number and Description of Network Telephones

Facility Information

- Platform/Site Description
- Number of Buildings
- Location

10.4.4.2 Meshing Information System Domains

Information services and applications provided to a subscriber require an interwoven framework of networks, data sources and applications spanning several information system domains. As illustrated in Figure 10-11, the ITSCs will mesh information system domains as necessary to identify the system chains needed to achieve enterprise capability. Using this method, ITSCs will be able to compare system characteristics and system behavior with mission effectiveness and system efficiency.

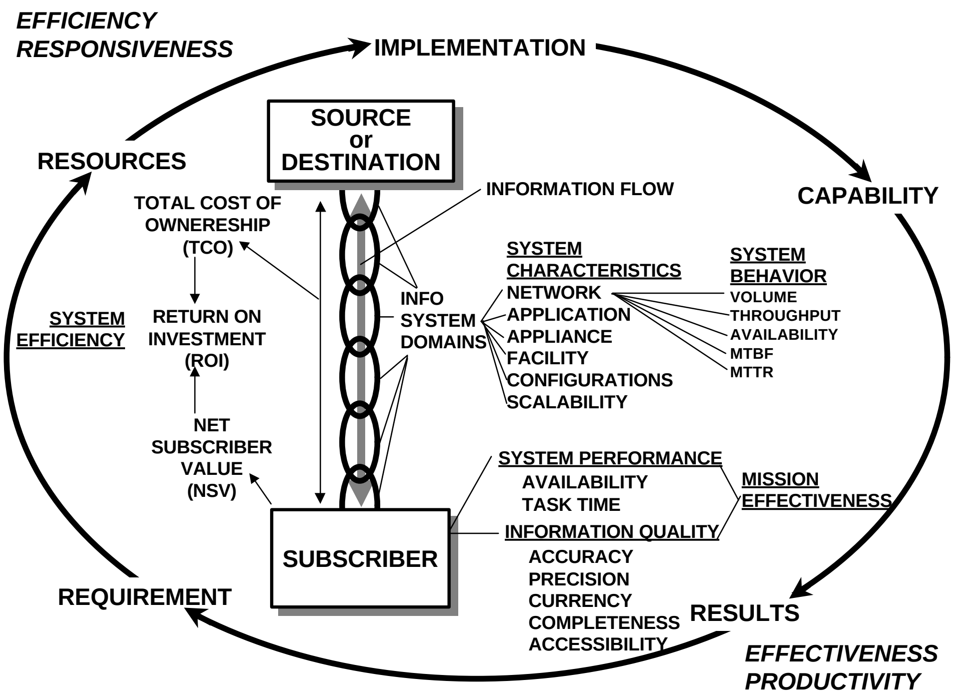

Figure 10-11. Summary of System Quality Measurements

10.4.4.3 Scalability

Scalability (SCA) is a measure of how easily a system can expand to meet an increased number of subscribers. For each operating system and software application associated with the capability, the maximum number of subscribers that an application or subsystem can support is tracked. For the chain of information systems associated with a system capability, or for an entire information system domain, the minimum value of all 'maximum subscribers per application or subsystem' becomes the scalability. In effect, scalability is the maximum number of users that can be supported.

Scalability is important to enterprise management because the Naval enterprise consists of nearly one million potential subscribers. Integrated information subsystems and components must be capable of meeting the full-scale requirements of the enterprise.

10.4.4.4 System Characteristics Summary

Table 10-8 provides a summary of system characteristics metrics as discussed above.

System Quality Measurement	Abbreviation	Unit of Measure	Measurer
Block Diagram	BD	Diagram	ITSC
Block Diagram of each information system domain within an area of coverage.			
System Identifying Information	SII	Descriptive Data	ITSC
Command Name, Domain Names, IP Addresses, ATM NSAP Addresses, Staff Code Schema, E-mail Address Schema			
Network Characteristics	NET	Diagrams & Descriptive Data	ITSC
External Interfaces, Topology, Diagram, Nodes, Net Diameter, Cable Plant, Protocols			
Application Characteristics	APPS	Descriptive Data	ITSC
Servers, Commercial Server Software, Government Server Software, VTC Servers			
Appliance Characteristics	APDV (Appliance Devices)	Descriptive Data	ITSC
Computer Clients, Commercial Client Software, Government Client Software, VTC Clients, Network Telephones			
Facility Characteristics	FAC	Diagrams & Descriptive Data	Command Consumer
Platform/Site Description, Number of Buildings, Locations of Facilities, Floor Plans, Power			
Scalability	SCA	Determination	ITSC
SCA = Minimum of (Maximum Subscriber of All System Components)			

Table 10-8. System Characteristics Metrics Summary

10.4.5 System Behavior

The fundamental system behaviors necessary to track the health of the infrastructure are as follows:

Storage Volume (VOL). Bytes currently being stored by a node or system component. It should be determined on an periodic basis and tracked for trend analysis and compared against the current situation. System behavior is often a function of the volume of information that it contains. Systems operating near capacity often exhibit abnormal symptoms.

Storage Capacity (CAP). The maximum volume that a system component can handle.

Throughput (TP). The number of bits per second that are transmitted or processed by a system component.

Throughput Rating (TP-R). The maximum number of bits per second that can be processed or transmitted by the system component at the physical layer.

Link Congestion (CG). Physical throughput divided by throughput rating.

Blocking (BK). Percent of time that a circuit cannot be established due to capacity being reached at a node.

Link Utility (UT). Number of different users or services attempting to use the link in a given period of time.

Availability (Ao). The amount of time that a system component is operating in an up status over the total elapsed time.

Mean Time Between Failures (MTBF). The average elapsed time between failures of a system component.

Mean Time To Repair (MTTR). The average elapsed time from the failure of a system component until its return to operation.

E-mail to No One (EMN). The measure of network and server response by sending an e-mail to no one between any two sites. The e-mail will bounce due to “no addressee found” and be returned to sender. The elapsed time from transmission to receipt of the non-delivery is a good measure of network and server loading as well as system faults.

System behavior is most easily measured on a component-by-component basis using the metrics described above. System behavior and system characteristics information can be used to identify areas where infrastructure improvement is needed. The ITSCs must collect and aggregate system behavior metrics and perform statistical analysis to investigate improvements in system performance and identify potential problem causes. Network modeling and simulation can be used to predict system behavior based upon proposed alternative changes in system characteristics.

Table 10-9 provides a summary of system behavior metrics discussed above.

System Quality Measurement	Abbreviation	Unit of Measure	Measurer
Volume	VOL	Bits	ITSC
Measured Value. Amount of bits currently present or stored in a system component or network node. For servers and computer clients this value can be expressed in bytes. Units must be specified.			
Capacity	CAP	Bits	ITSC
Value designated by the vendor, service provider or developer. Maximum amount of bits that can be present or stored in a system component or network node. For servers and computer clients this value can be expressed in bytes. Units must e specified.			
Throughput	TP	Bits per second	ITSC
Measured Value. Flow rate of processing rate of data. Can be physical or virtual (through compression)			
Rated Throughput	TP-R	Bits per second	ITSC
Value designated by the vendor or developer. Data rate or processing rate specified by the vendor, service provider or developer.			
Congestion	CG	Percent	ITSC
$CG = \frac{\text{Measured Physical Throughput on a Node or Link}}{\text{Rated Physical Throughput on a Node or Link}}$ Measurable by Network Analyzers or Circuit Analyzers			
Blocking	BK	Percent	ITSC
$BK = \frac{\text{Number of Calls or Circuits that get blocked due to lack of capacity on a switch}}{\text{Total Number of Calls or Circuits that are attempted. (measurable)}}$			
Utility	UT	Number per Minute	ITSC
UT = Number of users or services that attempt to use a system component over a period of time			
Availability	Ao	Percent	ITSC
$\frac{\text{Elapsed Time (month)} - \text{Down Time for a System Component or Object}}{\text{Elapsed Time (month)}}$			
Mean Time Between Failures	MTBF	Time (days)	ITSC
Calculated Value based on collected Data. Average lapsed time from one failure to the next for a system component or object. Important for trend analysis.			
Mean Time to Repair	MTTR	Time (hours)	ITSC
Calculated Value based on collected Data. Average lapsed time from failure to service return for a system component or object. Important for trend analysis.			
E-mail to No One	EMN	Time (seconds)	ITSC
Measured Value. Elapsed time from transmission of an e-mail to a non-existent address to receipt of the error notification from the destination e-mail server.			

Table 10-9. System Behavior Metrics Summary

10.4.6 Selection of Performance Metrics

Each of the metrics listed in sections 10.4.1 – 10.4.5 will be of varying degrees of utility to systems implementers and customers. Several concepts are useful in selecting which set of metrics to use from an enterprise organizational perspective.

10.4.6.1 IT Results Chain

The use of specific performance metrics should be aligned from the enterprise strategic plan via an IT/IM results chain. In other words, metrics should relate IT/IM outcomes to customer objectives, which are in turn related to enterprise program requirements. This helps one to focus on the metrics which truly support decision-making and program outcomes, and prevents optimization of individual customer results, to the detriment of the enterprise .

10.4.6.2 Balanced Scorecard

Performance metrics should be selected in such a way that they achieve a balance between both operational and strategic measures. Four generic goal areas include:

- Meeting the strategic needs of the enterprise
- Meeting the needs of individual operational users
- Addressing internal IT business performance (e.g., Total Ownership Cost; CDA performance; system metrics), and
- Addressing ongoing IT innovation and learning to achieve process improvement.

10.4.6.3 Targeted Measures

Organizations should match measures and performance results to the appropriate level of management/decision-making. These levels include DON, Regional, Command, and so forth. IT goals and measures should be included in IT performance improvement plans, and can even be tied to budgeting and procurement processes.

10.4.6.4 Comprehensive Measurement Capability

One should consider the way IT performance will be collected, analyzed, baselined, and benchmarked. One should select collection and analysis tools which will provide consistent indications of IT performance while automating the collection and analysis tasks as much as possible. The IT measurements and the process by which they are collected and analyzed should be periodically reviewed for appropriateness.

Note that these concepts are given as guidance on how to establish enterprise level performance measures. It is expected that in future releases of this ITSG, more detailed guidance will be provided on how to develop enterprise performance measurements and associated processes.

10.5 References

DOD Enterprise Management

Defense Information Systems Agency (DISA): Joint Defense Information Infrastructure Control Center Concept of Operations (DII CC CONOPS); 22 July 1997

Enterprise Management Metrics

Executive Guide: Measuring Performance and Demonstrating Results of Information Technology Investment; Exposure Draft; GAO/AIMD-97-163; General Accounting Office; http://www.gao.gov/policy/guidance.htm (Sep 97)

XSM

The Open Group (TOG) X/Open Systems Management, 6 July 1996; http://www.rdg.opengroup.org/public/pubs/catalog/t602.htm (24 May 1998)

Simple Network Management Protocol (SNMP)

Case (SNMP Research), Fedor, Schoffstell (Performance Management Inc.), Davin (MIT); "Simple Network Management Protocol (SNMP)" (IETF Standard 15/RFC-1157); May 1990: ftp://ftp.isi.edu/in-notes/rfc1157.txt (24 May 1998)

Rose (Performance Management Inc.), McCloghrie (Hughes LAN Systems) "Structure and Identification of Management Information for TCP/IP-based Internets" (IETF Standard 16/RFC-1155) , May 1990; ftp://ftp.isi.edu/in-notes/rfc1155.txt (24 May 1998)

Rose (Performance Management Inc.), McCloghrie (Hughes LAN Systems); "Concise MIB Definitions" (RFC-1212) March 1991; ftp://ftp.isi.edu/in-notes/rfc1212.txt (24 May 1998)

McCloghrie (Hughes LAN Systems), Rose (Performance Management Inc.); "Management Information Base for Network Management of TCP/IP-based internets: MIB-II" (IETF Standard 17/RFC-1213),March 1991, ftp://ftp.isi.edu/in-notes/rfc1213.txt (24 May 1998)

Waldbusser (Carnigie Mellon) , "Remote Network Monitoring Management Information Base", (RFC 1757) February 1995; ftp://ftp.isi.edu/in-notes/rfc1757.txt (24 May 1998)

Simple Network Management Protocol version 2 (SNMPv2)

Case (SNMP Research Inc.), McCloghrie (Hughes LAN Systems), Rose (Dover Beach Consultant Inc.), Waldbusser (Carnigie Mellon); Introduction to version 2 of the Internet-standard Network Management Framework (RFC 1441) April 1993RFC 1441, Simple Network Management Protocol Version 2, May 1993

Common Management Information Protocol

International Organization for Standardization (ISO) standard: ISO/IEC 9596-1/ITU-T X.711 "Common Management Information Protocol (CMIP)Specification;" 23 May 1998; http://www.iso.ch/cate/d29698.html (24 May 1998)

Remote Network Monitoring Version 2 (RMON2)

Waldbusser (INS), "Remote Network Monitoring Management Information Base Version 2 using SMIv2" (RFC 2021); January 1997; ftp://ftp.isi.edu/in-notes/rfc2021.txt (24 May 1998)

Biermen (Cisco), Iddon, (Axon Networks Inc.); "Remote Network Monitoring MIB Protocol Identifiers" (RFC 2074): January 1997 ftp://ftp.isi.edu/in-notes/rfc2074.txt (24 May 1998)

Web Based Enterprise Management (WBEM)

Free Range Media, Inc.; "Draft Proposal, WEBM" Version 0.4, 16 July 1996 http://wbem.freerange.com/new/wbem/obsm.htm (24 May 1998)

Intel Inc.; "Web Based Enterprise Management, Simplifying and Reducing the Cost of PC Ownership"; http://www.intel.com/managedpc/wbem/; (24 May 1998)

Duri, Weber (IBM Zurich Research Laboratory); "Webbin' CMIP," http://www.igd.fhg.de/www/www95/proceedings/posters/43/index.html (Jan 1998)

Desktop Management Interface (DMI)

Desktop Management Task Force (DMBF); Desktop Management Interface (DMI) Draft Proposal, DMI Version 2.0,29 March 1996 http://www/dmtf.org/ (24 May 1998)

ATM Forum Network Management Specification

ATM Forum web site: http://www.atmforum.com (30 May 1998)

International Telecommunications Union (ITU) Standards

International Telecommunications Union – Telecommunications (ITU-T); M.3000 Series of Recommendations on Telecommunications Management network (TMN) October 1997 http://www.itu.int/itudoc/itu-t/rec/m.html (24 May 1997)